

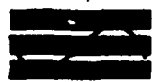
AD-A223 045

DTIC FILE COPY

ARO 24649.9-EL-S

(2)

A Novel Communication Network Simulator



Axiomatix

DTIC
ELECTE
JUN 20 1990
S B D

DISTRIBUTION STATEMENT A

Approved for public release;
Distribution Unlimited

90 06 18 265

2

A Novel Communication Network Simulator

Interim Technical Report

Prepared for

U.S Army Research Office
P. O. Box 12211
Research Triangle Park, NC 27709-2211

Contract No. DAAL 03-87-C-0007

Prepared by

Dr. Unjeng Cheng

Axiomatix
9841 Airport Blvd.
Suite 1130
Los Angeles, CA 90045

DTIC
ELECTE
JUN 20 1990
S B D

APPROVED FOR PUBLIC RELEASE
DISTRIBUTION LIMITED

The view, opinions, and/or findings contained in this report are those of the author(s) and should not be construed as an official department of the Army position, policy, or decision, unless so designated by other documentation.

Axiomatix Report No. R9003-3
March 31, 1990

REPORT DOCUMENTATION PAGE

1a. REPORT SECURITY CLASSIFICATION Unclassified		1b. RESTRICTIVE MARKINGS	
2a. SECURITY CLASSIFICATION AUTHORITY		3. DISTRIBUTION/AVAILABILITY OF REPORT Approved for public release; distribution unlimited.	
2b. DECLASSIFICATION/DOWNGRADING SCHEDULE			
4. PERFORMING ORGANIZATION REPORT NUMBER(S) R9003-3		5. MONITORING ORGANIZATION REPORT NUMBER(S) ARO 24649.9-EL-5	
6a. NAME OF PERFORMING ORGANIZATION Axiomatix	6b. OFFICE SYMBOL (if applicable)	7a. NAME OF MONITORING ORGANIZATION U. S. Army Research Office	
6c. ADDRESS (City, State, and ZIP Code) 9841 Airport Blvd., Suite 1130 Los Angeles, CA 90045		7b. ADDRESS (City, State, and ZIP Code) P. O. Box 12211 Research Triangle Park, NC 27709-2211	
8a. NAME OF FUNDING/SPONSORING ORGANIZATION U. S. Army Research Office	8b. OFFICE SYMBOL (if applicable)	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER DAAL03-87-C-0007	
8c. ADDRESS (City, State, and ZIP Code) P. O. Box 12211 Research Triangle Park, NC 27709-2211		10. SOURCE OF FUNDING NUMBERS	
		PROGRAM ELEMENT NO.	PROJECT NO.
		TASK NO.	WORK UNIT ACCESSION NO.
11. TITLE (Include Security Classification) A NOVEL COMMUNICATION NETWORK SIMULATOR			
12. PERSONAL AUTHOR(S) Unjeng Cheng			
13a. TYPE OF REPORT Interim	13b. TIME COVERED FROM TO	14. DATE OF REPORT (Year, Month, Day) 1990, March 31	15. PAGE COUNT 6
16. SUPPLEMENTARY NOTATION The view, opinions and/or findings contained in this report are those of the author(s) and should not be construed as an official Department of the Army position, policy, or decision, unless so designated by other documentation.			
17. COSATI CODES		18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number)	
FIELD	GROUP	SUB-GROUP	
		Direct-Sequence, Frequency-Hopping, Jamming, Networks, Packet Radio, Simulator, Spread-Spectrum	
19. ABSTRACT (Continue on reverse if necessary and identify by block number) This report presents the theoretical background of the Network Simulator, which is used for investigating the performance of communication networks under various jamming threats. To demonstrate the operation of a communication network under various jamming scenarios, we provide two spread-spectrum models: direct-sequence and frequency-hopping. The use of the spread-spectrum physical layer is to provide adequate anti-jamming capability. A salient feature of the Network Simulator is its capability to simulate the nonstationary jamming strategy. This is important because analytical models of nonstationary jamming do not exist.			
20. DISTRIBUTION/AVAILABILITY OF ABSTRACT <input checked="" type="checkbox"/> UNCLASSIFIED/UNLIMITED <input type="checkbox"/> SAME AS RPT. <input type="checkbox"/> DTIC USERS		21. ABSTRACT SECURITY CLASSIFICATION Unclassified	
22a. NAME OF RESPONSIBLE INDIVIDUAL Dr. Gaylord K. Huth		22b. TELEPHONE (Include Area Code) (213) 641-8600	22c. OFFICE SYMBOL

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE

TABLE OF CONTENTS

1. Introduction	1
2. Spread Spectrum Models	2
2.1 Direct-Sequence System	2
2.2 Frequency-Hopping System	3
3. Nonstationary Jamming Model	4



Accession For	
NTIS GRA&I	<input checked="" type="checkbox"/>
DTIC TAB	<input type="checkbox"/>
Unannounced	<input type="checkbox"/>
Justification _____	
By _____	
Distribution/	
Availability Codes	
Dist	Avail and/or Special
A-1	

1. Introduction

This report presents the theoretical background of the Network Simulator, which is used for investigating the performance of communication networks under various jamming threats. It has many useful features:

- (1) A network editor lets you create and edit the network easily.
- (2) A jammer editor lets you create and edit the jammers easily.
- (3) The route between any source-destination pair and the measured link quality can be displayed during simulation.
- (4) Two propagation loss models are provided, viz., the square-law loss and power-of-four loss models.
- (5) Two spread-spectrum models are provided, viz., the direct-sequence and frequency-hopping models.

Using this simulator, we are able to show that a fully-connected network may become partially connected when the jammer power is strong. This phenomena are more prominent for the power of four loss model than the square-law loss model. For the power-of-four loss model, the received signal and jamming power both decrease fast as the distance increases. Therefore, each jammer can only affect the nearby nodes and it is also more difficult for each communicator to talk to the jammed nodes far away from it.

We implemented the routing algorithm for the Packet-Radio (PR) network in the simulator since the algorithm is well-known and contains two important features:

- (1) automatic link quality measurement, and
- (2) automatic routing table computation.

The link quality measurement is done in two stages:

- (1) Each receiver keeps track of the number of correctly-received packets from each of its neighbors. Each transmitter keeps track of the number of packets transmitted to each of its neighbors.
- (2) When exchanging the routing information, the receiver notifies each of its neighbors of the number of correctly-received packets. The link is considered good if the percentage of the correctly-received packets exceeds 75%.

Note that for a fully-connected network without jamming, the routing algorithm will choose the one-hop operating scenario automatically. When the jammer is on, the algorithm will adopt the multi-hop operating scenario automatically if some links become bad.

2. Spread-Spectrum Models

To demonstrate the operation of a communication network under the various jamming scenarios, we provide two spread-spectrum models: direct-sequence and frequency-hopping. The use of the spread-spectrum physical layer is to provide adequate anti-jamming capability. Among various spread-spectrum systems and jamming techniques, we consider only two cases here. They are discussed in the following.

2.1 Direct-Sequence System

For the direct-sequence model, we assume the jammers are full-band noise jammer. The jammer k has the average jamming power J_k and it is on in a slot with probability $P_k^{(J)}$. For a node at distance r_k away from the jammer k , the received jamming power in a time slot is given by

$$J_k^{(R)} = \begin{cases} \frac{J_k}{r_k^m P_k^{(J)}} & \text{with probability } P_k^{(J)}, \\ 0 & \text{with probability } 1 - P_k^{(J)}, \end{cases}$$

where $m = 2$ for the square-law loss and $m = 4$ for the power of four loss.

We assume that all communicators have the same transmitting power S . The packet transmitted by node i will be received by node j with the signal power:

$$S_{ij}^{(R)} = \frac{S}{r_{ij}^m}$$

In this version of the Network Simulator, we assume BPSK modulation and no coding. Although we do reserve the data fields for the error correction code definition in the system parameters data form, the code is not used in the simulation.

There is a simple formula for computing the packet error probability in the DS model. The simulator can determine whether a received packet is received correctly without any symbol level manipulation. Therefore, we can use the real packet length in the simulation.

2.2 Frequency-Hopping System

The frequency-hopping model assumes the partial-band tone jamming and the M-ary Frequency-Shift-Keying (MFSK) modulation. We also assume there is one jamming tone per modulation band. Let F denote the fraction of the band being jammed. The jammer i has the average jamming power J_i and it is on in a slot with probability $P_i^{(J)}$. For a node at distance r_i away from the jammer i , the received jamming power in a time slot is given by

$$J_i^{(R)} = \begin{cases} \frac{J_i}{r_i^m P_i^{(J)} F} & \text{with probability } P_i^{(J)}, \\ 0 & \text{with probability } 1 - P_i^{(J)}, \end{cases}$$

where $m = 2$ for the square-law loss and $m = 4$ for the power-of-four loss. We assume that all communicators have the same transmitting power S . The packet transmitted by node i will be received by node j with the signal power:

$$S_{ij}^{(R)} = \frac{S}{r_{ij}^m}$$

The frequency-hopping receivers operate as follows: The largest and the second largest outputs among the M filters are selected. The ratio of the largest output to the second

largest output is compared to the threshold. If it is larger than 2, we accept the filter with the largest output. If the ratio is less than 2, we erase the symbol. An M-alphabet Reed-Solomon (RS) code is used to correct the errors and erasures.

Since there is no simple formula for computing the packet error probability. The FH model uses the symbol-by-symbol simulation: The simulator first determines that each received symbol is correct, erased, or wrong. Then it determines whether the received packet can be decoded successfully. The computation requirement for the FH model is significantly greater than the DS model. In order to simulate the network operation in a reasonable speed, we chose a short packet length for the FH model.

3. Nonstationary Jamming Model

A salient feature of the Network Simulator is its capability to simulate the nonstationary jamming strategy. A way to create a nonstationary jamming is to partition the time into blocks. Within each block of time, all jammers do not change their jamming power or jamming probability. One or more jammers can change their jamming power and/or jamming probability from block to block. This version of the Network Simulator allows you to define up to 10 jamming blocks. The duration of each block can be chosen arbitrarily. The simulator plays the jamming strategy repeatedly. When it starts, it begins with the first block and plays the blocks in the incremental order. After it finishes the last block, it goes back to the first block.